



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,720	02/09/2004	Xavier Boyen	ID-5	9562
36532	7590	06/23/2008	EXAMINER	
G. VICTOR TREYZ			DOAN, TRANG T	
FLOOD BUILDING				
870 MARKET STREET, SUITE 984			ART UNIT	PAPER NUMBER
SAN FRANCISCO, CA 94102			2131	
			MAIL DATE	DELIVERY MODE
			06/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/774,720	BOYEN, XAVIER	
	Examiner	Art Unit	
	TRANG DOAN	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 11 June 2004.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-19 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-19 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 09 February 2004 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ . |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>02/09/2004</u> . | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

1. Claims 1-19 are pending for consideration.

Priority

2. The application is filed on 02/09/2004 but claims the benefit of Provisional application has been made and acknowledged.

Drawings

3. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the informal drawings filed 2/9/2004 are difficult to read and not suitable for publication purposes. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Zheng (US 6396928) (hereinafter Zheng).

Regarding claim 1, Zheng discloses an identity-based-encryption (IBE) signcryption method in which a sender signs and encrypts a message M for a recipient, comprising: at the sender, digitally signing and encrypting a message M in a signcryption operation using an IBE private key of the sender SK^A and an IBE public key of the recipient ID^B that is based on the recipient's identity to generate a ciphertext C that is a signed and encrypted version of the message M (Zheng: column 7 lines 22-29 and column 13 lines 34-53); sending the ciphertext C to the recipient anonymously, wherein an attacker cannot deduce the authorship of the message from the ciphertext C (Zheng: column 1 lines 14-26); at the recipient, decrypting the ciphertext C using an IBE private key SK^B of the recipient that corresponds to the IBE public key ID^B , wherein decrypting the ciphertext produces an unencrypted version of the message M and an IBE public key of the sender ID^A that corresponds to the IBE private key SK^A (Zheng: column 14 lines 54-67); and at the recipient or at a third party, after the ciphertext has been decrypted by the recipient, performing signature verification in an operation that is separate from the decryption of the ciphertext, wherein performing the signature verification comprises using the decrypted message M and the IBE public key of the sender ID^A to prove that the sender signed the message M (Zheng: column 8 lines 12-14 and column 11 lines 25-42).

Regarding claim 2, Zheng further discloses wherein digitally signing and encrypting the message M comprises using the IBE private key SK^A in digitally signing the message M to produce digital signature information and using the IBE private key SK^A in encrypting at least a portion of the digital signature information (Zheng: column 9 lines 30-63).

Regarding claim 3, Zheng further discloses wherein using the IBE private key SK^A in digitally signing the message M comprises computing a commitment to a secret value and computing a corresponding decommitment (Zheng: column 9 lines 30-63).

Regarding claim 4, Zheng further discloses wherein using the IBE private key SK^A in encrypting the digital signature information comprises using the IBE private key to compute a symmetric key (Zheng: column 2 lines 64-67).

Regarding claim 5, Zheng further discloses comprising using the symmetric key to encrypt the message (Zheng: column 8 lines 55-64).

Regarding claim 6, Zheng further discloses comprising using the symmetric key to encrypt the IBE public key of the recipient, at least a portion of the digital signature information, and the message (Zheng: column 9 lines 30-63).

Regarding claim 7, Zheng further discloses wherein digitally signing and encrypting the message M in the signcryption operation comprises: computing a commitment to a secret value r and computing a corresponding decommitment; using the IBE private key SK^A in digitally signing the message M to produce digital signature information; and using the secret value r in encrypting the message M (Zheng: column 13 lines 34-67).

Regarding claim 8, Zheng further discloses wherein using the secret value r in encrypting the message M comprises using the secret value r to compute a symmetric key (Zheng: column 13 lines 34-67).

Regarding claim 9, Zheng further discloses comprising using the symmetric key to encrypt the message (Zheng: column 8 lines 55-64).

Regarding claim 10, Zheng further discloses comprising using the symmetric key to encrypt the IBE public key of the recipient, at least a portion of the digital signature information, and the message (Zheng: column 9 lines 30-63).

Regarding claim 11, Zheng further discloses wherein digitally signing and encrypting the message M comprises using the IBE private key SK^A in encrypting the message M (Zheng: column 13 lines 34-67).

Regarding claim 12, Zheng further discloses wherein digitally signing and encrypting the message comprises performing multiplication on an elliptic or hyperelliptic curve (Zheng: column 14 lines 43-54).

Regarding claim 13, Zheng discloses a method of signing and encrypting a message M comprising (Zheng: See Figs. 3-4 and column 13 lines 34-67): obtaining an identity-based-encryption (IBE) private key of a user; using the IBE private key to compute a commitment to a secret value and a corresponding decommitment (Zheng: See Figs. 3-4 and column 13 lines 34-67); and using a symmetric key that is based on the IBE private key to encrypt at least one of the commitment and the decommitment (Zheng: See Figs. 3-4 and column 13 lines 34-67).

Regarding claim 14, Zheng further discloses wherein using the symmetric key to encrypt comprises: concatenating the decommitment and the message (See Figs. 3-4 and column 13 lines 34-67); and using the symmetric key to encrypt the concatenated decommitment and message (See Figs. 3-4 and column 13 lines 34-67).

Regarding claim 15, Zheng further discloses wherein using the symmetric key to encrypt comprises: concatenating an IBE public key with the message and the decommitment (See Figs. 3-4 and column 13 lines 34-67); and using the symmetric key to encrypt the concatenated IBE public key, decommitment, and message (See Figs. 3-4 and column 13 lines 34-67).

Regarding claim 16, Zheng further discloses wherein computing the decommitment comprises performing multiplication on an elliptic or hyperelliptic curve (Zheng: column 14 lines 43-54).

Regarding claim 17, Zheng further discloses comprising computing the symmetric key that is based on the IBE private key by performing a bilinear pairing calculation on an elliptic or hyperelliptic curve (Zheng: column 14 lines 43-54).

Regarding claim 18, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Regarding claim 19, Zheng further discloses wherein sending the ciphertext C to the intended recipient anonymously comprises sending the ciphertext C to the intended recipient anonymously such that the attacker cannot deduce the authorship of the message from the ciphertext C (Zheng: column 13 lines 34-67).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131